UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

CARLOS HARDING, individually and on behalf of all others similarly situated, Plaintiff, v. MAXIMUS, INC. and MAXIMUS FEDERAL SERVICES, INC. Defendants.	Case No. 1:23-cv-1045 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Carlos Harding ("Plaintiff") individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, brings this Class Action Complaint against Defendants Maximus Federal Services, Inc. ("MFSI") and Maximus, Inc. ("Maximus" and collectively with MFSI, "Defendants"), and in support thereof alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action on behalf of himself and all other individuals ("class members"), totaling more than 11 million[1] people who had their sensitive personal identifiable information ("PII") and protected health information ("PHI")—as defined by the Health Insurance Portability and Accountability Act ("HIPPA")—accessed and hacked by malicious, unauthorized third parties that accessed and removed the PII and PHI from systems used by Defendants as early as May 27, 2023[2] (the "Data Breach").

[1] https://dataconomy.com/2023/08/01/maximus-data-breach-confirmed/ (last visited August 8, 2023).
[2] https://www.reuters.com/technology/hackers-use-flaw-popular-file-transfer-tool-steal-data-researchers-say-2023-06-02/ (last visited August 8, 2023); https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html (last visited August 8, 2023).

2. Defendants describe their business as a "leading operator of government health and human services programs and provider of technology solutions to governments," specializing in "business process services … in the health and human services markets."[3]

3. In the regular course of their business, Defendants use a file transfer service called MOVEit, marketed and offered by Progress Software Corporation ("PSC").[4]

4. Defendants tout the safety and security of their services on their website, www.maximus.com. For instance, Defendants' website states: "We are relentless in our pursuit to protect critical data, operations, and infrastructures. We go beyond traditional security measures to harden enterprise defenses for continuous mission protection."[5] These comments apply to third-party services that Defendants use in the ordinary course of its business, such as MOVEit.

5. Contrary to their assurances to consumers, however, Defendants lacked adequate systems and procedures for maintaining, safeguarding, and protecting highly sensitive PII and PHI entrusted to them. Specifically, on or about July 28, 2023, Defendants sent letters to class members, including Plaintiff, informing them that their highly sensitive PII and PHI were compromised in the Data Breach that impacted the MOVEit software.[6]

6. Based on Defendants' letters to class members such as Plaintiff, Defendants learned of the Data Breach on May 30, 2023, but inexplicably waited nearly two months before notifying class members that their highly sensitive PII and PHI were compromised thereby.

---

[3] MAXIMUS, INC., Form 10-K (FY 2022), https://investor.maximus.com/sec-filings/all-sec-filings/content/0001032220-22-000074/0001032220-22-000074.pdf (last accessed Aug. 4, 2023).
[4] MAXIMUS, INC., Form 8-K (July 26, 2023), https://www.sec.gov/ix?doc=/Archives/edgar/data/1032220/000103222023000061/mms-20230726.htm (last accessed Aug. 4, 2023).
[5] https://maximus.com/cybersecurity (last accessed Aug. 4, 2023).
[6] https://www.cms.gov/newsroom/press-releases/cms-responding-data-breach-contractor

7. It has been reported that the Data Breach was a ransomware attack conducted by a notorious ransomware group, C10p, which claims to have committed the Data Breach.[7]

8. As of July 19, 2023, it was reported that the Data Breach involved the theft of more than 37 million individuals' sensitive information, and more than 11 million consumers whose information was compromised by Defendants' use of MOVEit.[8]

9. Defendants owed a non-delegable duty to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII and PHI against unauthorized access and disclosure.

10. Defendants could have prevented the Data Breach by properly vetting and monitoring their systems and third party service providers, including MOVEit.

11. By way of example, had Defendants limited the customer information they shared with their vendors and business associates and/or employed reasonable measures to assure their vendors and business associates implemented and maintained adequate data security measures and protocols to secure and protect Plaintiff's and class members' data, the breach could have been prevented.

12. Plaintiff and class members entrusted Defendants with, and allowed Defendants to gather, highly sensitive information relating to their health and other matters as part of seeking medical treatment. They did so in confidence, and they had the legitimate expectation that Defendants would respect their privacy and act appropriately, including only sharing their information with vendors and business associates who legitimately needed the information and were equipped to protect it through having adequate processes in place to safeguard it.

---

[7] *Id.*

[8] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html

13. Trust and confidence are key components of Plaintiff's and class members' relationship with Defendants. Without it, Plaintiff and class members would not have provided Defendants with, or allowed Defendants to collect, their most sensitive information in the first place. To be sure, Plaintiffs and class members relied upon Defendants to keep their information secure, as they are required by law to do.

14. Defendants breached their non-delegable duties to class members by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII and PHI entrusted to it from unauthorized access and disclosure, including by ensuring their vendors and business associates had secure services, processes and procedures in place to safeguard PII and PHI that Defendants shared with those third-parties.

15. As a result of Defendants' breach of their non-delegable duties and obligations, the Data Breach occurred and Plaintiff's and class members' PII and PHI was accessed by, and disclosed to, an unauthorized third-party actor. This instant action seeks to remedy these failings and their consequences. Plaintiff thus brings this complaint on behalf of himself and all similarly situated individuals whose PII and/or PHI was exposed as a result of the Data Breach.

16. Plaintiff, on behalf of himself and all other class members, asserts claims for negligence, negligence per se, invasion of privacy, unjust enrichment, and violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1–201-9.3 ("UTPCPL") and seeks declaratory and injunctive relief, monetary damages including punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

A. Plaintiff

17. Plaintiff is a resident and citizen of the Commonwealth of Pennsylvania and resides in Stroudsburg, Pennsylvania.

18. Plaintiff received a letter from Defendants dated July 28, 2023, stating that his PII and PHI listed was impacted by the Data Breach and accessed by cybercriminals that accessed Defendants' systems:

- Name
- Social Security Number or Individual Taxpayer Identification Number
- Date of Birth
- Mailing Address
- Telephone Number, Fax Number, & Email Address
- Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
- Driver's License Number and State Identification Number
- Medical History/Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.)
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information
- Health Benefits & Enrollment Information

19. Prior to retaining counsel for claims related to the Data Breach, Plaintiff spent at least ten hours monitoring his accounts for fraudulent activity and identity theft. He will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint.

B. Defendants

20. Defendant Maximus, Inc. is a Virginia corporation, with its principal place of business in McLean, Virginia.

21. Defendant Maximus Federal Services, Inc. is a Virginia corporation, with its

principal place of business in McLean, Virginia. Maximus Federal Services, Inc. is a subsidiary of defendant Maximus, Inc.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000) and is a class action in which one or more class members are citizens of states different from Defendants.

23. The Court has general personal jurisdiction over Defendants because they maintain their headquarters and principal places of business in this judicial District (i.e., in McLean, Virginia), have minimum contacts with Virginia, and conduct substantial business in Virginia.

24. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in Virginia, Defendants maintain physical offices and principal places of business in this District, and because Defendants conduct a substantial part of their business within this District.

FACTUAL ALLEGATIONS

A. Overview of Defendants

25. Defendants' website promises consumers that Defendants have robust systems and processes in place to protect and secure their sensitive information:[9]

[9] https://maximus.com/cybersecurity (last accessed Aug. 4, 2023).

26. Defendants' website assures consumers—such as Plaintiff and class members—that Defendants are "expert[s]" in cybersecurity that offer a "full-spectrum cybersecurity services and technologies including cyber engineering and operations, threat hunting, pen testing, digital forensics, and incident response capabilities."[10]

27. Defendants claim that they can "help customers strengthen their cyber resiliency to protect critical data, operations and infrastructure for continual operational excellence and enhanced customer experiences."[11]

28. Defendants also state that in direct response to recent ransomware attacks, such as the Data Breach, they had taken additional steps to prevent such ransomware attacks from impacting their systems: "events of the past few years like the Colonial Pipeline ransomware attack have fueled a renewed focus on the importance of data security" such that entities should "think carefully about the workloads they are thinking of migrating when adopting cloud environments in order to ensure existing resources are a good option for the cloud." [12]

---

[10] *Id.*
[11] *Id.*
[12] MAXIMUS, INC., "The Cloud and Zero Trust: Finding the Right Balance" at p. 6, https://maximus.com/sites/default/files/documents/Federal/balancing-cloud-and-zero-trust-

29. Defendants' website repeatedly states that they are keenly cognizant of these data privacy risks and have adequate procedures and process in place to prevent them, including their statements that:

- "We strengthen cyber resiliency, protecting critical data, operations, and infrastructures for continual operational excellence. Our full-spectrum cybersecurity services offer unrivaled cyber defense against the most advanced cyber adversaries. From zero trust to secure application development, we deliver next-gen cyber technologies and solutions that address today's most complex security challenges."[13]

- "To defend against today's sophisticated cyber adversaries, Maximus goes beyond traditional security measures to harden enterprise security and continuously protect the mission."[14]

- "Maximus uses various technological and procedural security measures in order to protect the personal information we collect through the Site from loss, misuse, alteration or destruction. We have documented Information Security & Privacy policies to address data protection. We regularly provide information security and privacy awareness training to our employees."[15]

- "We have prepared a formal incident response plan in case of a data breach."[16]

- "Employees are provided a mandatory data privacy and security training webinar on an annual basis…We supplement the annual training with ongoing training provided through intranet articles and emails. Training topics include, but are not limited to the following: Data protection principles regarding the use, protection, storage, transmission, and disposal of confidential information, with specific focus on how certain data may not be used[.]"[17]

- "Maximus developed a robust incident management process to respond to a wide variety of cyber incidents globally. This process includes triage, investigation, evidence collection and storage, root cause analysis, and incident resolution with executive reporting."[18]

---

whitepaper.pdf (last accessed Aug. 4, 2023).

[13] https://maximus.com/technology-consulting-services (last accessed Aug. 4, 2023).

[14] https://maximus.com/cybersecurity (last accessed Aug. 4, 2023).

[15] MAXIMUS, INC., "Privacy Statement", https://maximus.com/privacy-statement (last accessed Aug. 4, 2023).

[16] *Id*

[17] MAXIMUS, INC., "Corporate Responsibility Report", MAXIMUS, INC., "Privacy Statement", https://maximus.com/privacy-statement (last accessed Aug. 4, 2023), 2023 (last accessed Aug. 4, 2023).f

[18] *Id.*

30. Defendants also tout their data security accreditations, including an ISO/IEC 20000-1 certification, and NCQA Accreditation.[19]

31. Based on the foregoing, Defendants were aware that they owed non-delegable duties to Plaintiff and class members to keep their PII and PHI safe and secure, which includes duties to ensure that all information Defendants collect, store and/or transfer is secure, and that any associated entities with whom Defendants shared information maintained adequate and commercially reasonable data security practices to ensure the protection of PII and PHI within Defendants' possession.

32. Discovery will show that through Defendants' provision of their services, they obtain possession of customers'—including Plaintiff's and class members'—highly sensitive PII and PHI. Thus, in the regular course of their businesses, Defendants collect and/or maintain the PII and PHI of consumers such as Plaintiff and class members. Upon information and belief, that information ordinarily includes: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) driver's license numbers or other state-issued ID numbers, (4) insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (5) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); (6) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by the provider); and (7) information of any parent, guardian, or guarantor. Defendants store this information digitally in the regular course of business.

[19] https://maximus.com/our-company (last accessed Aug. 4, 2023).

33. As evidenced by, *inter alia*, their receipt of the notice informing them that their PII and PHI were compromised in the Data Breach, Plaintiff's and class members' PII and/or PHI was transferred using MOVEit service and/or they otherwise entrusted to Defendants their PII and/or PHI, from which Defendants profited.

34. Yet, contrary to Defendants' website representations—by virtue of Defendants' admissions that they experienced the Data Breach which revealed the PII and PHI of more than 11 million individuals—Defendants did not have adequate measures in place to protect and maintain sensitive PII and PHI entrusted to them or to ensure their vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected consumers' PII and PHI that Defendants shared with third-party vendors such as PSC through Defendants' use of MOVEit.[20] Instead, Defendants' websites wholly fail to disclose the truth: that Defendants lack sufficient processes to protect the PII and PHI that is entrusted to them.

B. The Data Breach

35. On or about July 28, 2023, Defendants sent letters to class members, including Plaintiff, informing them that their highly sensitive PII and PHI were compromised in the Data Breach that impacted the MOVEit software[21]:

> Maximus Federal Services, Inc. (Maximus), are writing to inform you of an incident involving your personal information related to services provided by Maximus …. The incident involved a security vulnerability in the MOVEit software, a third-party application which allows for the transfer of files during the Medicare appeals process. Maximus is among the many organizations in the United States that have been impacted by the MOVEit vulnerability …. On May 30, 2023, Maximus detected unusual activity in its MOVEit application. Maximus began to investigate and stopped all use of the MOVEit application early on May 31, 2023. Later that same day, the third-party application provider, Progress Software Corporation, announced that a vulnerability in its MOVEit software had allowed an unauthorized party to gain access to files across many organizations in both the government and

[20] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html
[21] https://www.cms.gov/newsroom/press-releases/cms-responding-data-breach-contractor

> private sectors. Maximus notified CMS of the incident on June 2, 2023. To date, the ongoing investigation indicates that on approximately May 27 through 31, 2023, the unauthorized party obtained copies of files that were saved in the Maximus MOVEit application …. Maximus then began to analyze the files to determine which data had been affected. As part of that analysis, it was determined that those files contained some of your personal information …. We have determined that your personal and Medicare information was involved in this incident. This information may have included the following:
>
> - Name
> - Social Security Number or Individual Taxpayer Identification Number
> - Date of Birth
> - Mailing Address
> - Telephone Number, Fax Number, & Email Address
> - Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
> - Driver's License Number and State Identification Number
> - Medical History/Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.)
> - Healthcare Provider and Prescription Information
> - Health Insurance Claims and Policy/Subscriber Information
> - Health Benefits & Enrollment Information

36. Based on Defendants' letters to class members such as Plaintiff, Defendants learned of the Data Breach on May 30, 2023, but inexplicably waited nearly two months before notifying class members that their highly sensitive PII and PHI were compromised thereby.

37. Defendants' letter states that the breach originated through a compromise of PSC's MOVEit service. Defendants use MOVEit in the regular course of their business "for internal and external file sharing purposes, including to share data with government customers pertaining to individuals who participate in various government programs." MOVEit is a "managed file transfer software" that companies—such as Defendants—use to transfer files.[22]

[22] https://www.ipswitch.com/moveit?_ga=2.178322852.1251772019.1689781398-357640369.1688748444 (last visited August 1, 2023).

38. It has been reported by organizations using MOVEit software that were affected by the breach that PII and PHI were stolen, including name, address, SSN, birthdate, height, eye color, driver's license number, vehicle registration information, handicap placard information, clinical information, demographic information, and financial health information (such as insurance billing information), among others.[23] Upon information and belief, the information compromised in the Data Breach includes sensitive medical records and information related to health care and visits.

39. In an SEC Form 8-K statement filed after the Data Breach, Defendants stated that:

> On May 31, 2023, Progress Software Corporation, the developer of MOVEit ("MOVEit"), a file transfer application used by many organizations to transfer data, announced a critical zero-day vulnerability in the application that allowed unauthorized third parties to access its customers' MOVEit environments. It appears that a significant number of commercial and government customers worldwide were affected by this vulnerability. Maximus, Inc. ("Maximus" or the "Company") uses MOVEit for internal and external file sharing purposes, including to share data with government customers pertaining to individuals who participate in various government programs. The Company believes that the personal information of a significant number of individuals was accessed by an unauthorized third party by exploiting this MOVEit vulnerability…
>
> Based on the review of impacted files to date, the Company believes those files contain personal information, including social security numbers, protected health information and/or other personal information, of at least 8 to 11 million individuals to whom the Company anticipates providing notice of the incident.[24]

40. Thus, the Data Breach resulted from Defendants' failure to adequately protect and safeguard the highly sensitive PII and PHI entrusted to them, including by ensuring their vendors and business associates had secure services, processes and procedures in place to safeguard PII and PHI that Defendants shared with those third-parties.

---

[23] https://www.expresslane.org/alerts/ (last visited August 8, 2023).
[24] MAXIMUS, INC., Form 8-K (July 26, 2023), https://www.sec.gov/ix?doc=/Archives/edgar/data/1032220/000103222023000061/mms-20230726.htm (last accessed Aug. 4, 2023).

41. As noted above, it is believed that the Data Breach was a ransomware attack conducted by C10p, which itself claims to have committed the Data Breach.[25]

42. Through its hack of PSC's MOVEit service, C10p claims to have stolen PII and PHI information from over 550 organizations and 37 million individuals, including U.S. schools, the U.S. public sector, and the U.S. private sector.[26] C10p is a well-known ransomware group, which "[has] been linked to FIN11, a financially-motivated cybercrime operation" and is "connected to both Russia and Ukraine and which is believed to be part of a larger umbrella operation known as TA505."[27]

43. It has been reported that C10p has requested unspecified ransom from organizations impacted by the MOVEit Data Breach in exchange for C10p to abstain from releasing consumers' highly sensitive PII and PHI. As of July 19, 2023, C10p and its hacking of MOVEit has resulted in the theft of more than 37 million individuals' sensitive information.[28]

44. C10p posted a statement on its website demanding ransom from all companies impacted by the MOVEit breach, which includes the present Data Breach, stating that if they refused to pay the ransom, C10p would post the sensitive PII and PHI stolen from Defendants' systems on the dark web[29]:

---

[25] https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (last visited August 8, 2023).
[26] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html
[27] *Id*.
[28] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html
[29] *See supra* n.46.

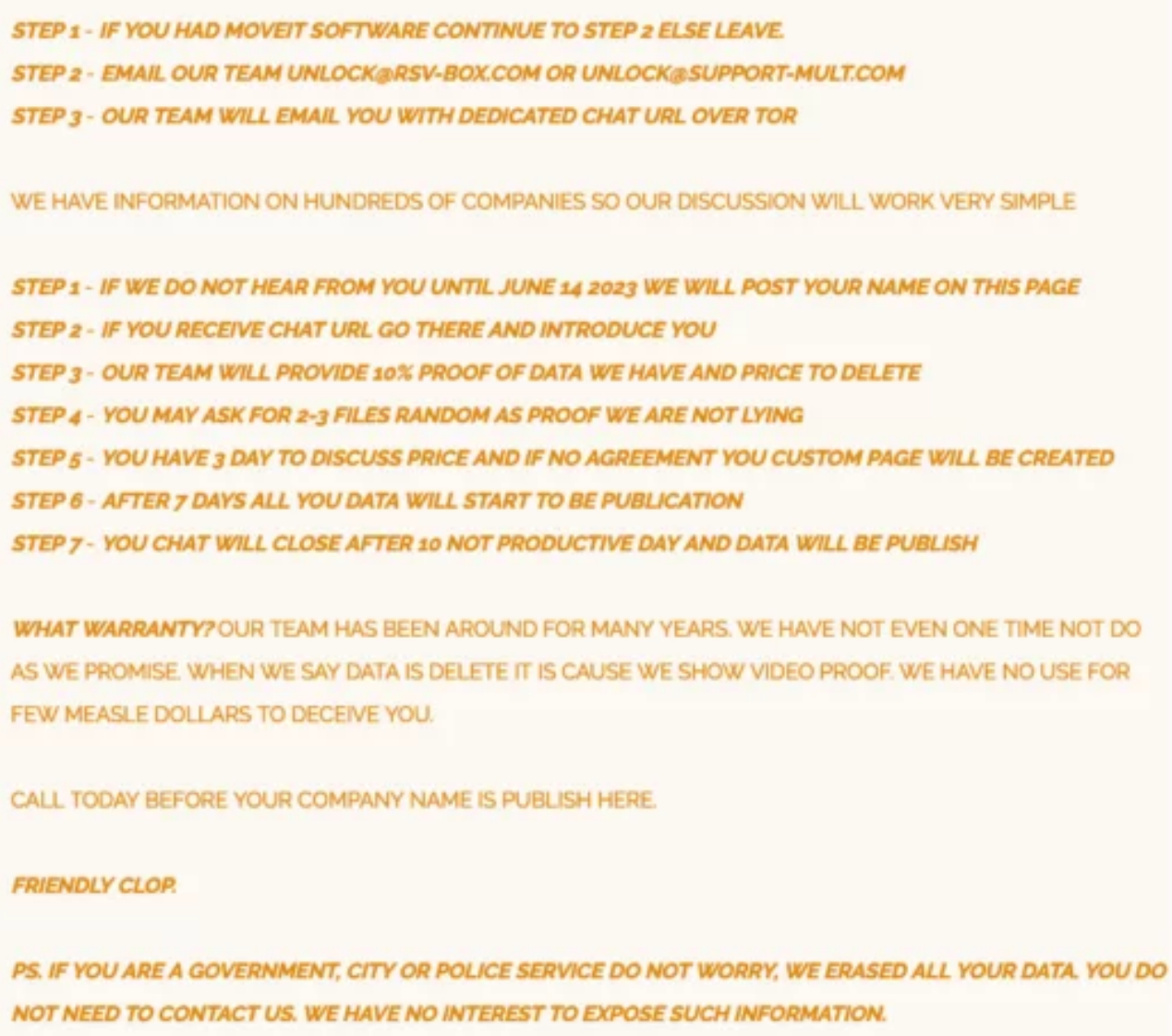
DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.



STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

45. Because the Data Breach was conducted by known, self-proclaimed ransomware cybercriminals, Plaintiff's and class members' sensitive PII and PHI are irrefutably in the possession of known bad actors. Furthermore, based on C10p's statement above, Plaintiff's and class members' PII and PHI may have already been published, which places them at imminent risk that their data will be misused.

46. As explicitly acknowledged and stated on their own websites, Defendants owed non-delegable duties to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII and PHI against unauthorized

access and disclosure, and to promptly notify individuals of any breach involving their information. Defendants breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect PII and PHI from unauthorized access and disclosure, including by ensuring its vendors and business associates had secure services, processes and procedures in place to safeguard PII and PHI that Defendants shared with those third-parties.

47. There were multiple things Defendants could have done—and were obligated to do—to ensure PSC (and the MOVEit service) had secure services, processes, and procedures in place to safeguard PII and PHI that Defendants provided to it, which would have prevented the Data Breach, but Defendants simply opted not to do them. For instance, as one leading cybersecurity expert explained, Defendants should have done the following when utilizing MOVEit. These steps, alongside others, could have ensured the sensitive PII and PHI Defendants transferred through MOVEit remained secure and free from data breach:

- "MOVEit should be behind technologies that provide access to only those who need it via tools such as Zero Trust (e.g. access gateways secured by MFA) or simple allowlists and blocklists."[30]
- "If you run MOVEit within your organization, ensure that the database runs as a specific user that can only interact with MOVEit and not as a superuser with broader access. The exploit utilizes SQL injection to allow attackers to manipulate server databases and execute arbitrary code, resulting in data exfiltration. Because this breach is an SQL injection leading to remote code execution (RCE), the

[30] https://securityscorecard.com/blog/three-steps-to-avoid-moveit-exploit/

adversary only gains initial access to the database server and user."[31]

Defendants also could have employed (either internally or through third parties) competent professionals to act as 24/7 "eyes on glass." Providers of managed security services, also referred to as "managed detection and response" ("MDR") employ a sophisticated series of artificial and human intelligence to monitor for signs that a breach is underway.

48. Either on their own or through the use of a qualified third-party vendor, Defendants could and should have been monitoring their own systems and repositories for indications of compromise ("IOCs.") It has been reported, for example, that the MOVEIT vulnerability was exploited by C10p "injecting" SQL computer code in order to execute a series of commands that ultimately resulted in the exfiltration of data. But companies have an obligation to monitor their systems for the execution of unauthorized code. If Defendant had had appropriate monitoring in place, it could have detected, and prevented this attack.

49. Companies who were using appropriate managed security detected the MOVEIT vulnerability as early as May 27, 2023, and were able to take steps to prevent the large scale exfiltration of consumers' sensitive information. For instance, on May 27, 2023, as part of C10P's attack of MOVEit, "Akamai researchers detected exploitation attempts against one of Akamai's financial customers — an attack that was blocked by the Akamai Adaptive Security Engine."[32] Thus, services were available for Defendants to detect the Data Breach and prevent large scale exfiltration of PII and PHI entrusted to Defendants, but Defendants simply failed to appropriately implement these services. Furthermore, it does not take cybersecurity expertise to know Defendants should not have maintained—or allowed the maintenance of—11 million consumers'

[31] *Id*.
[32] https://www.akamai.com/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware

PII and PHI on MOVEit software, where it was a sitting duck waiting for a cyberattack such as the Data Breach. In sum, there were plenty of technologies and processes readily available that Defendants could have utilized to prevent the Data Breach, but Defendants failed to do so.

C. Defendants Knew that Criminals Target PII and PHI

50. At all relevant times, Defendants knew, or should have known, the PII and PHI of individuals whose information was exfiltrated—such as Plaintiff and all other class members—were targets for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and class members' information from cyber-attacks that Defendants should have anticipated and guarded against.

51. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were 758 medical data breaches in 2020 with over 40 million patient records exposed.[33] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[34]

52. PII and PHI are valuable property rights.[35] The value of this information as a commodity is measurable.[36] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing

---

[33] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer (last accessed Nov. 15, 2021).
[34] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer (last accessed Nov. 15, 2021).
[35] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data
[36] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

legal and regulatory frameworks."[37] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[38] It is so valuable to identity thieves that once PII or PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

53. As a result of the real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII, PHI, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

54. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[39] A cyber-criminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[40] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[41]

---

[37] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[38] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[39] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[40] *Id.*

[41] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

55. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[42] According to a report released by the FBI's Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[43]

56. Criminals can use stolen PII and PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[44] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[45]

57. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[46]

---

[42] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[43] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[44] *What Happens to Stolen Healthcare Data*, *supra* at n.10.

[45] *Id.*

[46] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

58. Given these facts, any company that transacts business with a consumer and then compromises the privacy of that consumer's PII or PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Theft of PII and PHI Has Grave and Lasting Consequences for Victims

59. Theft of PII and PHI is serious. The FTC warns consumers that identity thieves use PII and PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[47]

60. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[48] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[49]

---

[47] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

[48] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[49] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

61. With access to an individual's PII or PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[50]

62. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[51]

63. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

64. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to

[50] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed August 8, 2023).
[51] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 15, 2021).

find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[52]

65. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[53] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[54] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII and PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[55] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[56]

66. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought or received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due

[52] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[53] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf
[54] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.14.
[55] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed August 8, 2023).
[56] *Id*.

to identity theft.

- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgages or other loans and may experience other financial impacts.

- Phantom medical debt collection based on medical billing or other identity information.

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[57]

67. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for a consumer to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[58]

68. It is within this harsh and dangerous reality that Plaintiff and all other class members must now live with the knowledge that their PII and PHI are forever in cyberspace and were taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

E. Damages Sustained by Plaintiff and the Other Class Members

69. Plaintiff and all other class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—a risk that justifies expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of

[57] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 24.
[58] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their PII and PHI permitted by Defendants; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; and/or (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

CLASS ALLEGATIONS

70. Plaintiff brings this action on behalf of himself and the following classes:

> Nationwide Class: All residents of the United States whose PHI and/or PII was compromised as a result of the Data Breach.
>
> Pennsylvania Subclass: All residents of Pennsylvania whose PHI and/or PII was compromised as a result of the Data Breach.

The foregoing classes are referred to herein, collectively, as the "Class." Excluded from the Class are: (1) the judges presiding over the action, Class Counsel, and members of their families; (2) the Defendants, their subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

71. **Numerosity**: Class members are so numerous that their individual joinder is impracticable, as the proposed Class includes at least 11 million members who are geographically dispersed.

72. **Typicality**: Plaintiff's claims are typical of class members' claims. Plaintiff and all class members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the class members he seeks to represent.

73. **Adequacy**: Plaintiff's interests are aligned with the Class he seeks to represent and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and his counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and undersigned counsel.

74. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other class members' claims. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Defendants' wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

75. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and class members' PII and PHI from unauthorized access and disclosure;

b. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and class members' PII and PHI;

c. Whether Defendants breached their duties to protect Plaintiff's and class members' PII and PHI;

d. Whether Defendants violated the statutes alleged herein;

e. Whether Plaintiff and all other class members are entitled to damages and the measure of such damages and relief.

76. Given that Defendants engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

77. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

78. Defendants owed duties to Plaintiff and all other class members to exercise reasonable care in safeguarding and protecting their PII and PHI in Defendants' possession, custody, or control, including non-delegable duties to safeguard that PII and PHI. This duty could not be delegated to Defendant's vendors and business associates; rather, Defendant had an independent obligation to control all environments into which it placed consumers' PII and PHI, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data.

79. Defendants owed duties to Plaintiff and class members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and class members' PII and

PHI within their control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

80. Defendants owed a duty of care to Plaintiff and class members to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the PII and PHI.

81. Defendants knew the risks of collecting and storing Plaintiff's and all other class members' PII and PHI and the importance of maintaining secure systems and ensuring their vendors and business associates with whom Defendants shared consumers PII and PHI—such as PSC through MOVEit—had secure services, processes and procedures in place to safeguard that PII and PHI. Defendants knew of the many data breaches that targeted healthcare providers in recent years.

82. Given the nature of Defendants' businesses, the sensitivity and value of the PII and PHI they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

83. Defendants breached their duties in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and class members' PII and PHI;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the PII and PHI at issue during the period of the Data Breach;

d. Failing to adequately monitor and audit the data security systems of its

vendors and business associates such as PSC (and the MOVEit service);

e. Failing to adequately monitor, evaluate, and ensure the security of PSC's network and systems;

f. Failing to recognize in a timely manner that Plaintiff's and class members' PII and PHI had been compromised; and

g. Failing to timely and adequately disclose that Plaintiff's and class members' PII and PHI had been improperly acquired or accessed.

84. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII and PHI by failing to control, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols to ensure that all software and hardware systems into which it placed consumers' data were protected against the unauthorized release, disclosure, and dissemination of Plaintiff's and class members' PII and PHI.

85. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and class members, their PII and PHI would not have been compromised.

86. As a result of Defendants' above-described wrongful actions, inactions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other class members have suffered, and will continue to suffer, economic damages and other injuries and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk that justifies expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; (v) lost value of the unauthorized

access to their PII and PHI permitted by Defendants; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; and/or (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

87. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

88. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

89. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure PII and PHI.

90. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other class members' PII and PHI and not complying with applicable industry standards, including by failing to control all environments into which it placed consumers' PII and PHI, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI

they obtain and store, and the foreseeable consequences of a data breach involving PII and PHI including, specifically, the substantial damages that would result to Plaintiff and the other class members.

91. Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence per se.

92. Plaintiff and class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

93. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

94. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and class members' PII and PHI to unauthorized individuals.

95. The injury and harm that Plaintiff and the other class members suffered was the direct and proximate result of Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; (v) lost

value of the unauthorized access to their PII and PHI permitted by Defendants; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; and/or (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT III
INVASION OF PRIVACY
(INTRUSION UPON SECLUSION)
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

96. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

97. Plaintiff and class members had a reasonable expectation of privacy in the PII and PHI that Defendants failed to safeguard and allowed to be accessed by way of the Data Breach.

98. Defendants' conduct as alleged above intruded upon Plaintiff's and class members' seclusion under common law.

99. By intentionally and/or knowingly failing to keep Plaintiff's and class members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiff's and class members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and class members' private affairs in a manner that identifies Plaintiff and class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and class members.

100. Defendants knew that an ordinary person in Plaintiff's and a class member's position would consider Defendants' intentional actions highly offensive and objectionable.

101. Defendants invaded Plaintiff and class members' right to privacy and intruded into Plaintiff's and class members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

102. Defendants intentionally concealed from Plaintiff and class members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

103. As a proximate result of such intentional misuse and disclosures, Plaintiff's and class members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendants' conduct, amounting to a substantial and serious invasion of Plaintiff's and class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

104. In failing to protect Plaintiff's and class members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and class members' rights to have such information kept confidential and private.

105. As a direct and proximate result of the foregoing conduct, Plaintiff seeks an award of damages on behalf of himself and the Class.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

106. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

107. Plaintiff and class members have both a legal and equitable interest in their PHI and PII that was collected by, stored by, and maintained by Defendants—thus conferring a benefit upon Defendants—that was ultimately compromised by the Data Breach.

108. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and class members. Defendants also benefitted from the receipt of Plaintiff's and class members' PHI and PII.

109. As a result of Defendants' failure to safeguard and protect PII and PHI, Plaintiff and class members suffered actual damages.

110. Defendants should not be permitted to retain the benefit belonging to Plaintiff and class members because Defendants failed to adequately implement the data privacy and security procedures that were mandated by federal, state, and local laws and industry standards.

111. Defendants should be compelled to provide for the benefit of Plaintiff and class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT V
DECLARATORY RELIEF
(28 U.S.C. § 2201)
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

112. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

113. An actual controversy has arisen and exists between Plaintiff and class members, on the one hand, and Defendants on the other hand, concerning the Data Breach and Defendants' failure to protect Plaintiff's and class members' PHI and PII, including with respect to the issue of whether Defendants took adequate measures to protect that information. Plaintiff and the Class are entitled to judicial determination as to whether Defendants have performed and are adhering to all

data privacy obligations as required by law or otherwise to protect Plaintiff's and class members' PHI and PII from unauthorized access, disclosure, and use.

114. A judicial determination of the rights and responsibilities of the parties regarding Defendants' privacy policies and whether they failed to adequately protect PHI and PII is necessary and appropriate to determine with certainty the rights of Plaintiff and the Class, and so that there is clarity between the parties as to Defendants' data security obligations with respect to PHI and PII going forward, in view of the ongoing relationships between the parties.

COUNT VI
VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW ("UTPCPL")
73 P.S. §§ 201-1–201-9.3
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Pennsylvania Subclass)

115. Plaintiff realleges and incorporates by reference paragraphs 1 through 76 as if fully set forth herein.

116. Defendants sell and perform services in the Commonwealth of Pennsylvania.

117. Plaintiff, class members, and Defendants are "persons" as defined by the UTPCPL. 73 P.S. § 201-2(2).

118. Defendants' services constitute as "trade" and "commerce" under the statute. 73 P.S. § 201-2(3).

119. Defendants obtained Plaintiff's and class members' PII/PHI in connection with the services they perform and provide.

120. Defendants engaged in unfair or deceptive acts in violation of the UTPCPL by failing to implement and maintain reasonable security measures to protect and secure consumers' (such as Plaintiff's and class members') PII/PHI in a manner that complied with applicable laws, regulations, and industry standards, including by failing to control all environments into which it

placed consumers' PII and PHI, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data.

121. As alleged above, Defendants make explicit statements to their customers that their PII/PHI will remain private and secure.

122. The UTPCPL lists twenty-one instances of "unfair methods of competition" and "unfair or deceptive acts or practices." 73 P.S. § 201-2(4). Defendants' failure to adequately protect Plaintiff's and class members' PII/PHI while holding out that it would adequately protect the PII/PHI falls under at least the following categories:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that he does not have (73 P.S. § 201-2(4)(v));

b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another (73 P.S. § 201-2(4)(vii));

c. Advertising goods or services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)); and

d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

123. Due to the Data Breach, Plaintiff and class members have lost property in the form of their PII/PHI. Further, Defendants' failure to adopt reasonable practices in protecting and safeguarding their customers' PII/PHI will force Plaintiff and class members to spend time or money to protect against identity theft. Plaintiff and class members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

124. As a result of Defendants' violations of the UTPCPL, Plaintiff and class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased or imminent risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their PII and PHI permitted by Defendants; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (viii) overpayment for the services that were received without adequate data security.

125. Pursuant to 73 P.S. § 201-9.2(a), Plaintiff seeks actual damages, $100, or three times their actual damages, whichever is greatest. Plaintiff also seeks costs and reasonable attorney fees.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as Class Representative and undersigned counsel as Class Counsel;

B. Award Plaintiff and the Class actual and statutory damages, punitive damages, nominal damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and the Class such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: August 8, 2023

Respectfully submitted,

/s/ Steven T. Webster

Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP
300 N. Washington Street, Ste. 404
Alexandria, Virginia 22314
Tel: (888) 987-9991
swebster@websterbook.com

E. Michelle Drake (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE, PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
Email: emdrake@bm.net

Mark B. DeSanto (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604

Email: mdesanto@bm.net

Norman E. Siegel (*Pro Hac Vice* forthcoming)
Barrett J. Vahle (*Pro Hac Vice* forthcoming)
J. Austin Moore (*Pro Hac Vice* forthcoming)
Jillian R. Dent (*Pro Hac Vice* forthcoming)
Brandi S. Spates (*Pro Hac Vice* forthcoming)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com
dent@stuevesiegel.com
spates@stuevesiegel.com

Attorneys for Plaintiff